SWGDE Capture of Live Systems

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Capture of Live Systems

Table of Contents

1. Purpose

The purpose of this document is to provide guidance to the forensic community on acquiring data from live computer systems. A primary concern is the ability to capture and save data in a usable format. Factors such as the volatility or the volume of data, restrictions imposed by legal authority, or the use of encryption may dictate the need to capture data from systems without interrupting the power cycle.

2. Scope

This paper provides guidance and considerations for the acquisition of data from live computer systems which may include volatile memory and/or data from mounted file systems as stored in a computer.

3. Order of Volatility

When acquiring evidence, the examiner must carefully consider the order in which data is collected due to its potential volatility and the effect of the collection on the system. This order may change based upon the system. The examiner must understand the needs of the given situation and order the collection of volatile data accordingly.

One example order of volatility is:

1. RAM
2. Running processes
3. Network connections
4. System settings
5. Storage media

4. Technical Details

There are four categories of live acquisitions:

1. Live memory (RAM, pagefile, swapfile, etc.)
2. Volatile system data/processes
3. Live file/file system acquisition
4. Live physical acquisition

4.1 Live Memory

Live memory acquisition methods copy data currently residing in system memory. Generally, live acquisition methods require administrator-level privileges for the system. The time required to extract all data from a system may contribute to the condition known as memory smear, where data is modified during the acquisition process.

4.2 Volatile system data/processes

Volatile system data collection utilizes the execution of commands or batch scripts to collect ephemeral information regarding the current system, such as: running processes, network connections, passwords, file system status, open sockets, connected users, etc. Best practice dictates the use of trusted binaries for this purpose, when available.

4.3 Live file/file system acquisition

A live file/file system acquisition permits the examiner to acquire data that may not be accessible once the system has been shut down, such as: mounted encryption containers, network storage, databases, etc. As encryption may prevent access to data after shutdown, the file system should be acquired live. Additionally, unsaved open files should be collected while the system is live.

4.4 Live Physical Acquisition

Situations may dictate that a system be acquired physically without shutting it down. This acquisition method is susceptible to data smear caused by file access during the acquisition process.

5. Tools and Training

Several tools exist to capture system memory from a computer system. Most solutions are software based, require little training to successfully capture system memory, and require local administrator rights for most modern operating systems.

6. Limitations

The examiner should be aware that interacting with a live computer system will cause changes to the system. The examiner should know that their actions may cause changes to the data (e.g., RAM) and risk causing system instability. The examiner should understand these concerns and how they may apply to their particular situation. The examiner must take measures to keep the system accessible for the duration of the acquisition process. Given that the examiner is working with volatile data, the examiner should maintain detailed documentation of all actions taken.

SWGDE Capture of Live Systems

History

Revision	Issue Date	Section	History
0.1	03/06/2007	All	Document created by Standards and Accreditation Committee. Original Release for Public Comments.
1.0	01/28/2008	All	Final Release
2.0	06/06/2014	All	Rewrite/Technical refresh. Voted to release as a Draft for Public Comment.
2.0	06/12/2014	Disclaimer/ All	Formatted for publishing as a Draft for Public Comment.
2.0	08/28/2014	None	No changes made; voted to publish as an Approved document.
2.0	09/05/2014	All	Formatting and technical edit performed for release as an Approved document.